

REMARKS

In the Official Action mailed on **May 20, 2004**, the examiner reviewed claims 25-51. Claims 25, 34, and 43 were rejected under 35 U.S.C. §103(a) as being unpatentable over Zizzi (USPN 6,185,681, hereinafter "Zizzi") in view of McBride (USPN 6,292,899 B1, hereinafter "McBride"). Claims 26-28, 30-33, 35-37, 39-42, 44-46, and 48-51 were rejected under 35 U.S.C. §103(a) as being unpatentable over Zizzi in view of McBride, and further in view of Sutter (USPN 5,924,094, hereinafter "Sutter"). Claims 29, 38, and 47 were rejected under 35 U.S.C. §103(a) as being unpatentable over Zizzi in view of McBride, and further in view of Sutter, and further in view of Brogliatti et al. (USPN 6,564,225 B1, hereinafter "Brogliatti").

Rejections under 35 U.S.C. §103(a)

Independent claims 25, 34, and 43 were rejected as being unpatentable over Zizzi in view of McBride. Applicant respectfully points out that McBride teaches **generating a checksum of the encryption instruction code** in the cipher engines and on the lock-out instructions to detect alteration of the instruction code (see McBride, col. 6, lines 11-24). Zizzi is silent concerning creating a digest of the data.

In contrast, the present invention is directed to creating a digest that is a **cryptographic function of the data** to detect tampering with the data (see page 8, lines 4-21 of the instant application). Creating a digest that is a cryptographic function of the data is beneficial because it provides a cryptographically secure method for detecting tampering with the data. The system of McBride generates a checksum of the encryption instruction code to detect alteration of the instruction code, but does not provide a means for detecting tampering with the data. Moreover, the use of a checksum fails to meet the security standards of a digest that is a cryptographic function of the data,

because a checksum is typically less secure and easier to compromise. There is nothing within Zizzi or McBride, either separately or in concert, which suggests creating a digest that is a cryptographic function of the data to detect tampering with the data.

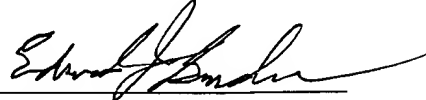
Accordingly, Applicant has amended independent claims 25, 34, and 43 to clarify that the present invention creates a digest that is a cryptographic function of the data to detect tampering with the data. These amendments find support on page 8, lines 4-21 of the instant application

Hence, Applicant respectfully submits that independent claims 25, 34, and 43 as presently amended are in condition for allowance. Applicant also submits that claims 26-33, which depend upon claim 25, claims 35-42, which depend upon claim 34, and claims 44-51, which depend upon claim 43, are for the same reasons in condition for allowance and for reasons of the unique combinations recited in such claims.

CONCLUSION

It is submitted that the present application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By 
Edward J. Grundler
Registration No. 47, 615

Date: June 9, 2004

Edward J. Grundler
PARK, VAUGHAN & FLEMING LLP
508 Second Street, Suite 201
Davis, CA 95616-4692
Tel: (530) 759-1663
FAX: (530) 759-1665